REMARKS

The present Amendment amends claims 1, 3-9, and 11-16, cancels claim 2, and leaves claim 10 unchanged. Therefore, the present application has pending claims 1 and 3-16.

35 U.S.C. §102 Rejections

Claims 1, 3-7 and 16

Claims 1-7 and 16 stand rejected under 35 U.S.C. §102(e) as being anticipated by U. S. Patent Publication No. 2003/0174718 to Sampath et al. ("Sampath"). As previously indicated, claim 2 was canceled. Therefore, this rejection regarding claim 2 is rendered moot. Regarding the remaining claims 1, 3-7 and 16, this rejection is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 1, 3-7 and 16 are not taught or suggested by Sampath whether taken individually or in combination any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Amendments were made to the claims to more clearly describe features of the present invention. Specifically, amendments were made to the claims to more clearly recite that the present invention is directed to a network authentication apparatus, a network authentication system and a network apparatus as recited, for example, in independent claims 1 and 16.

The present invention, as recited in claim 1, and a similarly recited in claim 16, provides a network authentication apparatus. The network authentication apparatus includes a network interface unit connected with a network and that transmits/receives a packet. The network authentication apparatus also includes a packet relay unit that relays a received packet in accordance with a destination

13

address of the received packet. Further, the network authentication apparatus

includes a filtering processing unit that extracts one or more of a destination MAC

(Media Access Control) address and a destination IPv6 (Internet Protocol version 6)

address and a source MAC address, and that extracts only an interface ID part of a

source IPv6 address contained in the received packet, and that determines whether

to relay the received packet to the packet relay unit or discard the packet in

accordance with: one or more of the destination MAC address and the destination

IPv6 address and the source MAC address; and only the interface ID part of the

source IPv6 address extracted from the received packet. The prior art does not

disclose all of these features.

The above described features of the present invention, as now more clearly

recited in the claims, are not taught or suggested by any of the references of record,

particularly Sampath, whether taken individually or in combination with any of the

other references of record.

Sampath teaches a scalable packet filter for a network device. However,

there is no teaching or suggestion in Sampath of the network authentication

apparatus, the network authentication system, or the network apparatus as recited in

claims 1 and 16 of the present invention.

Sampath discloses a network device for network communications. The

device includes at least one data port interface, where the at least one data port

interface supports at least one data port transmitting and receiving data and a CPU

interface, and where the CPU interface is configured to communicate with a CPU.

The network device also includes a memory communicating with the at least one

data port interface, a memory management unit, the memory management unit

including a memory interface for communicating data from the at least one data port

14

interface and the memory and a communication channel, the communication

channel for communicating data and messaging information between the at least

one data port interface, the CPU interface, the memory, and the memory

management unit. The network device also includes a fast filtering processor, the

fast filtering processor filtering packets coming into the at least one data port

interface, and taking selective filter action on a particular packet of the packets

based upon specified packet field values. The specified packet field values are

obtained by applying a filter mask, obtained from a field table, to the particular packet

and the selective filter action is obtained from a policy table based on the specified

packet field values.

One feature of the present invention, as recited in claim 1, and as similarly

recited in claim 16, includes a filtering processing unit that extracts one or more of a

destination MAC (Media Access Control) address and a destination IPv6 (Internet

Protocol version 6) address and a source MAC address, and that extracts only an

interface ID part of a source IPv6 address contained in the received packet, and that

determines whether to relay the received packet to the packet relay unit or discard

the packet in accordance with: one or more of the destination MAC address and the

destination IPv6 address and the source MAC address; and only the interface ID part

of the source IPv6 address extracted from the received packet. Sampath does not

disclose this feature.

When a terminal device of a certain user moves and the network to be

connected is changed, the terminal device newly receives distribution of an IP

address from a DHCP (dynamic host configuration protocol) server, at the

destination network. Therefore, the IP address of the terminal device changes when

the terminal device moves. In some cases, the IP address cannot be used as a

15

parameter of user authentication and filtering. It is an object of this invention to solve the matter described above. It is another object of this invention to secure both mobility and security in a system where user authentication and filtering are performed. (*See, e.g.*, page 3, line 23 to page 4, line 4 in the specification).

The present invention focuses on an interface ID, which is in the lower 64 bits of an IPv6 address, which is ID proper to the terminal device, and which is an invariant ID even when the network to be connected is changed. A feature of the present invention includes using the interface ID as a parameter of user authentication and filtering. Accordingly, the present invention has a great advantage in that it is possible to secure both mobility and security in a system where user authentication and filtering are performed.

Specifically, in the present invention, the interface ID part which is the lower 64 bits of the IPv6 address is used rather than the network ID part, which is the upper 64 bits of the IPv6 address. The interface ID part is used because the network ID part would change in accordance with a movement of the terminal device. As described, for example, on page 15, line 17 to page 16, line 9 and page 33, lines 7-15, the present invention as now more clearly recited in the claims, provides where only the interface ID part of the source IPv6 address is extracted, and where it determined whether to relay a packet or discard the packet based on the extracted interface ID part – not based on the network ID part.

Sampath relates to a network device including a filtering processor which would filter packets based on a MAC address and an IP address. However, Sampath does not disclose mobility of a terminal at all. For example, Sampath discloses a source IP address in a field table (*see, e.g., paragraphs* [0051] and [0052]; and TABLE 3). There is no teaching or suggestion in Sampath of an

16

interface ID of a source IPv6 address (i.e., a source IPv6 interface ID). When the

source IP address of Sampath is used for filtering, even if the address is an IPv6

address, it is not possible to secure mobility because the source IP address includes

a network ID (refer to Fig.7 of the present invention). Accordingly, Sampath does not

have the purpose or an advantage of securing mobility as in the present invention.

Sampath also discloses "User Defined 16 bit field" in the TABLE 3. However,

the "User Defined 16 bit field" is different from the 64 bits interface ID of the source

IPv6 address of the present invention. Accordingly, Sampath does not set the

interface ID of the source IPv6 address in the field, and is quite different from the

present invention.

In the Response to the Arguments, the Examiner acknowledges Applicants'

assertion that the source IPv6 interface ID is the lower 64 bits of the IPv6 address.

Based on this, the Examiner asserts that when Sampath is filtering according to the

source IP address, it is also filtering according to the source IPv6 interface ID (*see,*

e.g., page 2, paragraph 4). However, as previously discussed, filtering according to

the source IP address (both the network ID and the interface ID) and filtering

according to the interface ID part of the source IP address (i.e., not based on the

network ID) are different, particularly with regard to the advantages of mobility and

security. Accordingly, the present invention is quite different from Sampath.

Therefore, Sampath fails to teach or suggest "<u>a filtering processing unit that</u>

<u>extracts one or more of a destination MAC (Media Access Control) address and a</u>

<u>destination IPv6 (Internet Protocol version 6) address and a source MAC address,</u>

<u>and that extracts only an interface ID part of a source IPv6 address contained in the</u>

<u>received packet, and that determines whether to relay the received packet to the</u>

<u>packet relay unit or discard the packet in accordance with: one or more of the</u>

17

destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address extracted from the received packet" as recited in claim 1, and as similarly recited in claim 16

Therefore, Sampath does not teach or suggest the features of the present invention, as recited in claims 1, 3-7 and 16. Accordingly, reconsideration and withdrawal of the 35 U.S.C. §102(e) rejection of claims 1, 3-7 and 16 as being anticipated by Sampath are respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references used in the rejection of claims 1, 3-7 and 16.

Claims 1, 3-8 and 11-16

Claims 1-8 and 11-16 stand rejected under 35 U.S.C. §102(b) as being anticipated by U. S. Patent Publication No. 2002/0016858 to Sawada et al. ("Sawada"). As previously indicated, claim 2 was canceled. Therefore, this rejection regarding claim 2 is rendered moot. Regarding the remaining claims 1, 3-8 and 11-16, this rejection is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 1, 3-8 and 11-16 are not taught or suggested by Sawada, whether taken individually or in combination any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Amendments were made to the claims to more clearly describe features of the present invention. Specifically, amendments were made to the claims to more clearly recite that the present invention is directed to a network authentication

18

apparatus, a network authentication system and a network apparatus as recited, for example, in independent claims 1, 11 and 16.

The present invention, as recited in claim 1, and as similarly recited in claims 11 and 16, provides a network authentication apparatus. The network authentication apparatus includes a network interface unit connected with a network and that transmits/receives a packet. The network authentication apparatus also includes a packet relay unit that relays a received packet in accordance with a destination address of the received packet. Further, the network authentication apparatus includes a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address extracted from the received packet. The prior art does not disclose all of these features.

The above described features of the present invention, as now more clearly recited in the claims, are not taught or suggested by any of the references of record, particularly Sawada, whether taken individually or in combination with any of the other references of record.

Sawada teaches a communication apparatus for routing or discarding a packet sent from a user terminal. However, there is no teaching or suggestion in Sawada of the network authentication apparatus, the network authentication system, or the network apparatus as recited in claims 1, 11 and 16 of the present invention.

19

Sawada discloses a packet communications apparatus. The apparatus includes a plurality of network interfaces (NIFs), a learned address table, a packet forwarding unit (PFU) and a processor for directive packets to change state (PDPCS). The learned address table contains information for identifying a NIF through which to send a packet. The PFU selects a port through which to forward a packet by referring to the learned address table, according to the state of the NIFs, and forwards or discards a packet received from a user terminal. The PDPCS receives a packet including a directive to change the state of a specific NIF to one of the connected state, disconnected state and stateless. The PDPCS changes the state of the specific NIF to one of the connected state, disconnected state and stateless, according to the directive in the packet.

One feature of the present invention, as recited in claim 1, and as similarly recited in claims 11 and 16, includes a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address extracted from the received packet. Sawada does not disclose this feature.

As previously discussed, the present invention focuses on an interface ID, which is the lower 64 bits of an IPv6 address. This ID is an invariant ID even when the network to be connected is changed. One feature of the present invention is to use the interface ID as a parameter of user authentication and filtering. Thereby, the

20

present invention has a great advantage that it is possible to secure both mobility and security in a system where user authentication and filtering are performed.

Sawada discloses a packet communication apparatus that performs an authentication and secures security based on a MAC address and an IP address. However, Sawada is not directed to the mobility of a terminal, and does not disclose extracting only the interface ID part of the source IPv6 address and determining whether to relay the packet or discard the packet based on the extracted interface ID part – not based on the network ID part – as in the present invention. Accordingly, the present invention distinguishes over Sawada.

Therefore, Sawada fails to teach or suggest "a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address extracted from the received packet" as recited in claim 1, and as similarly recited in claims 11 and 16

Therefore, Sawada does not teach or suggest the features of the present invention, as recited in claims 1, 3-8 and 11-16. Accordingly, reconsideration and withdrawal of the 35 U.S.C. §102(b) rejection of claims 1, 3-8 and 11-16 as being anticipated by Sawada are respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references used in the rejection of claims 1, 3-8 and 11-16.

35 U.S.C. §103 Rejections

Claims 8, 9 and 11-15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Sampath in view of U. S. Patent No. 6,442,588 to Clark et al. ("Clark"). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention, as now more clearly recited in claims 8, 9 and 11-15, are not taught or suggested by Sampath or Clark, whether taken individually or in combination with each other in the manner suggested by the Examiner. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Claims 8 and 9 are dependent on claim 1. Therefore, Applicants submit that claims 8 and 9 are allowable for at least the same reasons as previously discussed regarding independent claim 1.

Regarding the remaining claims 11-15, amendments were made to the claims to more clearly describe features of the present invention. Specifically, amendments were made to the claims to more clearly recite that the present invention is directed to a network authentication system as recited, for example, in independent claim 11.

The present invention, as recited in claim 11, provides a network authentication system. The network authentication system includes an authentication server that receives an authentication request from an arbitrary information terminal device connected via a network, and that executes authentication based on predetermined information received from the arbitrary information terminal device. The network authentication system also includes a network node device connected to the network and that relays a packet received from the network.

22

According to the present invention, the network node device includes: a network interface unit connected with the network and that transmits/receives a packet; a packet relay unit that relays a received packet in accordance with a destination address of the received packet; and a filtering processing unit. The filtering processing unit extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address received from the received packet,.

Also according to the present invention, the filtering processing unit determines a condition for a determination of whether to relay or to discard based on the authentication result by the authentication server, and the filtering processing unit relays only a packet addressed to the authentication server to the packet relay unit, of packets sent from an arbitrary information terminal device that is not authenticated by the authentication server. The prior art does not teach or suggest all of the above-described features.

The above-described features of the present invention, as now more clearly recited in the claims, are not taught or suggested by any of the references of record. Specifically, the features are not taught or suggested by either Sampath or Clark, whether taken individually or in combination with each other.

23

As previously discussed, Sampath teaches a scalable packet filter for a network device. However, there is no teaching or suggestion in Sampath of the network authentication system as recited in claim 11 of the present invention.

One feature of the present invention, as recited in claim 11, includes a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address received from the received packet. Sampath does not disclose this feature.

As previously discussed, when a terminal device of a certain user moves and the network to be connected is changed, the terminal device newly receives distribution of an IP address from a DHCP (dynamic host configuration protocol) server, at the destination network. Therefore, the IP address of the terminal device changes when the terminal device moves. In some cases, the IP address cannot be used as a parameter of user authentication and filtering. It is an object of this invention to solve the matter described above. It is another object of this invention to secure both mobility and security in a system where user authentication and filtering are performed. (See, e.g., page 3, line 23 to page 4, line 4 in the specification).

Also, as previously discussed, the present invention focuses on an interface ID, which is in the lower 64 bits of an IPv6 address, which is ID proper to the terminal device, and which is an invariant ID even when the network to be connected is changed. A feature of the present invention includes using the interface ID as a

24

parameter of user authentication and filtering. Accordingly, the present invention has a great advantage in that it is possible to secure both mobility and security in a system where user authentication and filtering are performed.

Specifically, in the present invention, the interface ID part which is the lower 64 bits of the IPv6 address is used rather than the network ID part, which is the upper 64 bits of the IPv6 address. The interface ID part is used because the network ID part would change in accordance with a movement of the terminal device. As described, for example, on page 15, line 17 to page 16, line 9 and page 33, lines 7-15, the present invention as now more clearly recited in the claims, provides where only the interface ID part of the source IPv6 address is extracted, and where it determined whether to relay a packet or discard the packet based on the extracted interface ID part – not based on the network ID part.

As previously discussed, Sampath relates to a network device including a filtering processor which would filter packets based on a MAC address and an IP address. However, Sampath does not disclose mobility of a terminal at all. For example, Sampath discloses a source IP address in a field table (*see, e.g., paragraphs* [0051] and [0052]; and TABLE 3). There is no teaching or suggestion in Sampath of an interface ID of a source IPv6 address (i.e., a source IPv6 interface ID). When the source IP address of Sampath is used for filtering, even if the address is an IPv6 address, it is not possible to secure mobility because the source IP address includes a network ID (refer to Fig.7 of the present invention). Accordingly, Sampath does not have the purpose or an advantage of securing mobility as in the present invention.

Sampath also discloses "User Defined 16 bit field" in the TABLE 3. However, the "User Defined 16 bit field" is different from the 64 bits interface ID of the source

IPv6 address of the present invention. Accordingly, Sampath does not set the interface ID of the source IPv6 address in the field, and is quite different from the present invention.

In the Response to the Arguments, the Examiner acknowledges Applicants' assertion that the source IPv6 interface ID is the lower 64 bits of the IPv6 address. Based on this, the Examiner asserts that when Sampath is filtering according to the source IP address, it is also filtering according to the source IPv6 interface ID (*see, e.g.,* page 2, paragraph 4). However, as previously discussed, filtering according to the source IP address (both the network ID and the interface ID) and filtering according to the interface ID part of the source IP address (i.e., not based on the network ID) are different, particularly with regard to the advantages of mobility and security. Accordingly, the present invention is quite different from Sampath.

Therefore, Sampath fails to teach or suggest "a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address received from the received packet" as recited in claim 11.

The above noted deficiencies of Sampath are not supplied by any of the other references of record, namely Clark, whether taken individually or in combination with each other. Therefore, combining the teachings of Sampath and Clark in the manner

26

suggested by the Examiner still fails to teach or suggest the features of the present invention as now more clearly recited in the claims.

Clark teaches a method of administering a dynamic filtering firewall. However, there is no teaching or suggestion in Clark of the network authentication system as recited in claim 11 of the present invention.

Clark discloses a method of permitting a subscriber access to an online server complex operated by a particular online service provider (OSP). An IP communication request including a destination IP address and an origination IP address is received. The IP communication request is forwarded to a dynamic filtering firewall if the destination IP address corresponds to a service provided by the particular OSP. The origination IP address is compared with a table of stored authenticated IP addresses. The IP communication request is forwarded to the destination IP address if the origination IP address matches an IP address contained in the table.

One feature of the present invention, as recited in claim 11, includes a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address received from the received packet. Clark does not disclose this feature, and the Examiner does not rely upon Clark for teaching a filtering processing unit.

Therefore, Clark fails to teach or suggest "a filtering processing unit that extracts one or more of a destination MAC (Media Access Control) address and a destination IPv6 (Internet Protocol version 6) address and a source MAC address, and that extracts only an interface ID part of a source IPv6 address contained in the received packet, and that determines whether to relay the received packet to the packet relay unit or discard the packet in accordance with: one or more of the destination MAC address and the destination IPv6 address and the source MAC address; and only the interface ID part of the source IPv6 address received from the received packet" as recited in claim 11.

Both Sampath and Clark suffer from the same deficiencies, relative to the features of the present invention, as recited in the claims. Therefore, combining the teachings of Sampath and Clark in the manner suggested by the Examiner does not render obvious the features of the present invention as now more clearly recited in the claims. Accordingly, reconsideration and withdrawal of the 35 U.S.C. §103(a) rejection of claims 8, 9 and 11-15 as being unpatentable over Sampath in view of Clark are respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references used in the rejection of claims 8, 9 and 11-15.

Claim 10 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Sampath and further in view of U. S. Patent No. 7,051,365 to Bellovin. Claim 10 is dependent on claim 1. Therefore, claim 10 is allowable for at least the same reasons previously discussed regarding independent claim 1.

In view of the foregoing amendments and remarks, Applicants submit that claims 1 and 3-16 are in condition for allowance. Accordingly, early allowance of claims 1 and 3-16 is respectfully requested.

To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing Attorney Docket No. HAS-101).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

/DONNA K. MASON/
Donna K. Mason
Registration No. 45,962

DKM/jab
(703) 684-1120